

# PATENT ABSTRACTS OF JAPAN

(1)Publication number : 2002-290396

(43)Date of publication of application : 04.10.2002

(51)Int Cl

H04L 9/16  
H04L 9/08

(21)Application number : 2001-085823

(71)Applicant : TOSHIBA CORP

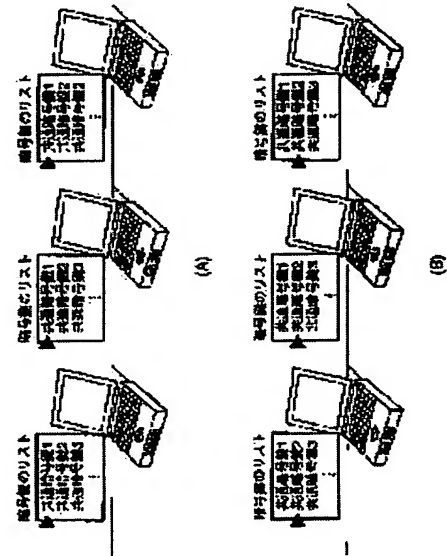
(22)Date of filing : 23.03.2001

(72)Inventor : SUZUKI NOBORU

## 64) ENCRYPTION KEY UPDATE SYSTEM AND ENCRYPTION KEY UPDATE METHOD

(57)Abstract:

**PROBLEM TO BE SOLVED** : To provide an encryption key update system that can synchronously update encryption keys of all devices transmitting/receiving data without the need for users to make troublesome works such as entry of the encryption key and settings.  
**SOLUTION** : The encryption key update system has distributed an encryption key list on which a plurality of encryption keys are described in advance to all devices encrypting data by using a common encryption key system, and also distributed a program to select one encryption key or more in the encryption key list on the basis of a prescribed rule to each device. For example, each device selects a 'common encryption key 1' for a period as an encryption key and automatically sets it to a communication environment. After that, each device aborts the 'common encryption key 1' on the border of a date and time and selects a 'common encryption key 2' for the encryption key and automatically sets it to the communication environment.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-290396

(P2002-290396A)

(43) 公開日 平成14年10月4日 (2002.10.4)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	キーワード (参考)
H 0 4 L 9/16		H 0 4 L 9/00	6 4 3 5 J 1 0 4
9/08			6 0 1 E

審査請求 未請求 請求項の数10 O L (全 9 頁)

(21) 出願番号 特願2001-85823(P2001-85823)

(22) 出願日 平成13年3月23日 (2001.3.23)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 鈴木 昇

東京都青梅市末広町2丁目9番地 株式会  
社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム (参考) 5J104 AA01 AA16 AA34 EA04 EA24

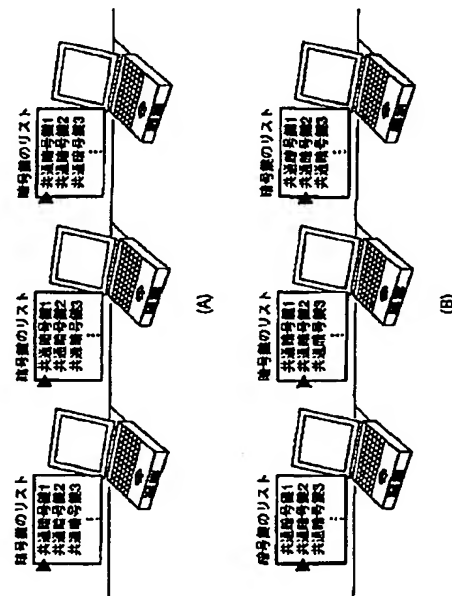
JA03 NA02 PA07

(54) 【発明の名称】 暗号鍵更新システムおよび暗号鍵更新方法

(57) 【要約】

【課題】 ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システム。

【解決手段】 この暗号鍵更新システムでは、共通暗号鍵方式によるデータの暗号化を行うすべての装置に、予め複数の暗号鍵が記された暗号鍵リストを配布しておく。また、各装置には、所定の規則に基づき、この暗号鍵リストの中から1つ以上の暗号鍵を選択するプログラムも配布しておく。そして、たとえば、ある期間、各装置は、「共通暗号鍵1」を暗号鍵として選択し、それを通信環境に自動設定する。その後、ある日時を境に、各装置は、その「共通暗号鍵1」を破棄して「共通暗号鍵2」を暗号鍵として選択し、それを通信環境に自動設定する。



## 【特許請求の範囲】

【請求項1】 暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いにデータを送受信する通信システムの暗号鍵更新システムであって、

前記各装置が、複数の暗号鍵が記された電子的な暗号鍵リストを保持するリスト保持手段と、

予め定められた規則に基づき、前記リスト保持手段に保持された暗号鍵リストに記される複数の暗号鍵の中から1つ以上の暗号鍵を選択する選択手段とを具備したことを特徴とする暗号鍵更新システム。

【請求項2】 前記各装置が、予め定められた規則に基づき、前記選択手段により選択された暗号鍵の有効期間を算出する有効期間算出手段と、

前記選択手段により暗号鍵が選択された時から前記有効期間算出手段により算出された期間が経過した時に、前記選択手段に新たな暗号鍵を選択させる暗号鍵更新手段とを具備したことを特徴とする請求項1記載の暗号鍵更新システム。

【請求項3】 前記選択手段は、前回選択した暗号鍵の中の少なくとも1つを再度選択することを特徴とする請求項1または2記載の暗号鍵更新システム。

【請求項4】 前記各装置が、前記選択手段により暗号鍵が選択された時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加える時差調整手段を具備することを特徴とする請求項1または2記載の暗号鍵更新システム。

【請求項5】 前記各装置が、前記暗号鍵リストを受信するリスト受信手段と、前記リスト保持手段に保持された暗号鍵リストを前記リスト受信手段により受信された暗号鍵リストに更新するリスト更新手段とを具備することを特徴とする請求項1、2、3または4記載の暗号鍵更新システム。

【請求項6】 暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いにデータを送受信する通信システムの暗号鍵更新方法であって、

前記各装置が、複数の暗号鍵が記された電子的な暗号鍵リストを保持するステップと、

予め定められた規則に基づき、前記保持した暗号鍵リストに記される複数の暗号鍵の中から1つ以上の暗号鍵を選択するステップとを有することを特徴とする暗号鍵更新方法。

【請求項7】 前記各装置が、予め定められた規則に基づき、前記選択された暗号鍵の有効期間を算出するステップと、前記暗号鍵を選択した時から前記算出された期間が経過

した時に、新たな暗号鍵を選択するステップとを有することを特徴とする請求項6記載の暗号鍵更新方法。

【請求項8】 前記選択ステップは、前回選択した暗号鍵の中の少なくとも1つを再度選択することを特徴とする請求項6または7記載の暗号鍵更新方法。

【請求項9】 前記各装置が、前記暗号鍵を選択した時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加えるステップを有することを特徴とする請求項6または7記載の暗号鍵更新方法。

【請求項10】 前記各装置が、前記暗号鍵リストを受信するステップと、前記保持した暗号鍵リストを前記受信した暗号鍵リストに更新するステップとを有することを特徴とする請求項6、7、8または9記載の暗号鍵更新方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、たとえば無線通信回線を介してデータを送受信する通信システムの暗号鍵更新システムおよび暗号鍵更新方法に係り、特に、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システムおよび暗号鍵更新方法に関する。

## 【0002】

【従来の技術】近年、データ通信技術の向上は目覚ましく、インターネットやイントラネットなどと称される通信システムが急速に普及している。また、最近では、赤外線や電波などによりデータを送受信する無線通信を利用した無線LAN (Local Area Network) をオフィス内に構築する企業も多くなってきている。この無線LANは、ケーブルの敷設を必要としないために、たとえば組織の改編に伴うオフィス内のレイアウト変更などにも柔軟に対応することが可能である。

【0003】赤外線や電波などにデータを搬送させる無線通信では、その漏洩を発生させ易いため、有線通信以上に、第三者によるデータの傍受や改ざん等を防ぐための対策が重要視される。このことから、従来より、データの暗号化という手法が広く採用されている。このデータの暗号化は、(1) 共通暗号鍵方式、(2) 公開暗号鍵方式のいずれか、あるいは、この2つの組み合わせによるものが現在のところ主流である。

【0004】共通暗号鍵方式は、送信側(データを暗号化する側)と受信側(暗号化されたデータを復号する側)とが、予め共通の暗号鍵を持ち、この同一の暗号鍵を用いて暗号化および復号を行う方式である。一方、公開暗号鍵方式は、ある鍵から公開鍵と秘密鍵との2種類の鍵を生成し、公開鍵を予め送信側に配布しておく。そして、送信側は、この公開鍵を用いてデータを暗号化し、受信側は、この公開鍵と対になっている秘密鍵で復

号を実行する。また、この共通暗号鍵方式と公開暗号鍵方式との組み合わせは、共通暗号鍵方式における共通暗号鍵を公開暗号鍵方式によって授受するものである。

【0005】このように、共通暗号鍵や公開鍵、秘密鍵を用いてデータの暗号化および復号を行うことにより、データの傍受や改ざんを防止することが可能となる。

【0006】また、最近では、社内LANに外出先等の遠隔地からアクセスしたいといった要望も多く、これに答えるために、たとえば加国ボーダー・ネットワーク・テクノロジー社や米国セキュリティダイナミクス社等がワンタイム・パスワード・システムと称されるユーザ認証システムを開発するに至っている。

【0007】このワンタイム・パスワード・システムは、データを暗号化するものではないが、遠隔地からアクセスするユーザが正規のユーザかどうかを確認することによってネットワークのセキュリティを高めるためのシステムであり、たとえばネットワーク側のファイア・ウォールとモバイルコンピュータに接続される拡張ユニットなど、アクセスされる側とアクセスする側とで同じ時に同じ乱数を発生させる仕組みを持たせる。そして、ユーザは、たとえば1分ごとに発生・更新される乱数をパスワードとしてその拡張ユニットの入力装置に入力し、そのパスワードの承認を条件に、そのネットワークへのアクセスが許可される。

【0008】つまり、このワンタイム・パスワード・システムでは、各パスワードがいわゆる使い捨てであるため、パスワードの盗難を考慮する必要がない。

【0009】

【発明が解決しようとする課題】ところで、前述した共通暗号鍵方式によるデータの暗号化では、同じ鍵を長期間に渡って使い続けると、その暗号が破られる危険性が高くなってしまふ。したがって、ある期間ごとに鍵を更新する作業が必要となってくる。

【0010】しかしながら、たとえばIEEE802.11b規格における無線LANの暗号鍵は、40ビット以内や128ビット以内での設定が可能であり、128ビットからなる暗号鍵を新たに配布・設定しようとする、その作業は非常に煩雑である。そして、人手を介することから、たとえば設定ミスや暗号鍵自体の漏洩を誘発するおそれがあった。

【0011】また、公開暗号鍵方式によるデータの暗号化や、共通暗号鍵方式と公開暗号鍵方式との組み合わせによる暗号化では、ハードウェアやファームウェアなど、ネットワークの下位層に処理をさせるには複雑すぎて実現困難であり、また、仮に実現できたとしても通信性能が著しく低下してしまうといった問題があった。

【0012】一方、ワンタイム・パスワード・システムは、利用の度にパスワードを変える方式であるため、共通暗号鍵方式によるデータの暗号化のように、ある期間ごとに鍵を更新するという作業は一切不要である。し

かし、このワンタイム・パスワード・システムも、システムが発生させる乱数をその都度ユーザに入力させなければならないといった同様の問題を抱えている。

【0013】この発明はこのような事情を考慮してなされたものであり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システムおよび暗号鍵更新方法を提供することを目的とする。

【0014】

【課題を解決するための手段】前述した目的を達成するために、この発明は、たとえば1年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたものである。そして、そのために、この発明は、暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いに情報を送受信する通信システムの暗号鍵更新システムであって、前記各装置が、複数の暗号鍵が記された電子的な暗号鍵リストを保持するリスト保持手段と、予め定められた規則に基づき、前記リスト保持手段に保持された暗号鍵リストに記される複数の暗号鍵の中から1つ以上の暗号鍵を選択する選択手段とを具備したことを特徴とする暗号鍵更新システムを提供する。

【0015】この発明の暗号鍵更新システムにおいては、所定の規則に基づき、各装置が予め与えられた複数の暗号鍵の中から暗号化および復号に用いる暗号鍵を選択するため、その結果として、すべての装置が同期を取って暗号鍵を自動的に更新することが可能となり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることがない。

【0016】また、この発明の暗号鍵更新システムは、前記各装置が、予め定められた規則に基づき、前記選択手段により選択された暗号鍵の有効期間を算出する有効期間算出手段と、前記選択手段により暗号鍵が選択された時から前記有効期間算出手段により算出された期間が経過した時に、前記選択手段に新たな暗号鍵を選択させる暗号鍵更新手段とを具備することが好ましい。これにより、暗号鍵の更新サイクルに不規則性を持たせることができ、セキュリティをより向上させることが可能となる。

【0017】また、この発明の暗号鍵更新システムは、前記選択手段が、前回選択した暗号鍵の中の少なくとも1つを再度選択することが好ましい。これにより、たとえば更新前と更新後とで少なくとも1つは合致することになり、暗号鍵の更新時にもデータの送受信を中断させることがない。

【0018】また、この発明の暗号鍵更新システムは、前記各装置が、前記選択手段により暗号鍵が選択された

10

20

30

40

50

時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加える時差調整手段を具備することが好ましい。これにより、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収することが可能となる。

【0019】また、この発明の暗号鍵更新システムは、前記各装置が、前記暗号鍵リストを受信するリスト受信手段と、前記リスト保持手段に保持された暗号鍵リストを前記リスト受信手段により受信された暗号鍵リストに更新するリスト更新手段とを具備することが好ましい。これにより、最初に暗号鍵リストを配布してシステムを起動させた後は、この暗号鍵リスト自体を暗号化して授受することができるようになり、以降、ユーザによる暗号鍵リストの配布や設定などを一切不要とすることが可能となる。

【0020】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。

【0021】図1は、この発明の実施形態に係る暗号鍵更新システムが適用される通信システムのネットワーク構成図である。

【0022】図1に示すように、この通信システムは、有線LAN100にネットワーク管理サーバコンピュータ1と複数のアクセスポイント2とが接続される。また、各アクセスポイント2は、赤外線や電波などを利用して、パーソナルコンピュータ3との間に無線通信路を確立する。

【0023】ネットワーク管理サーバコンピュータ1は、この通信システム全体の管理を司るものであり、後述する暗号鍵リストの配布などを実行する。また、アクセスポイント2は、パーソナルコンピュータ3を有線LAN100に接続するための装置であり、パーソナルコンピュータ3と同じ暗号鍵を保有し、この暗号鍵でデータの暗号化と復号とを行いながら、つまり共通暗号鍵方式による暗号化を行いながらパーソナルコンピュータ3との間でデータを送受信する。

【0024】このアクセスポイント2とパーソナルコンピュータ3との双方に共有される暗号鍵は、たとえば4つまで一時に設定可能であり、複数の暗号鍵が設定された場合、送信側は、その中のどれかをを用いて暗号化を行う。この時、送信側は、何番目の暗号鍵を使用したかを示す情報をパケットに格納して転送する。一方、受信側は、このパケットに格納された情報で示される番号の暗号鍵を用いて復号を実行する。

【0025】そして、この通信システムに適用される暗号鍵更新システムは、このアクセスポイント2とパーソナルコンピュータ3との双方に共有される暗号鍵を、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、同期的に更新できるようにした点特徴としており、以下、この点について詳述する。

【0026】図2は、この暗号鍵更新システムで実行される暗号鍵の更新の概要を示すための概念図である。

【0027】この暗号鍵更新システムでは、共通暗号鍵方式によるデータの暗号化を行うすべての装置、より具体的には、ここでは、すべてのアクセスポイント2およびパーソナルコンピュータ3に、予め複数の暗号鍵が記された暗号鍵リストを配布しておく。そして、各装置には、所定の規則に基づき、この暗号鍵リストの中から1つ以上の暗号鍵を選択するプログラムも配布しておく。

【0028】たとえば図2(A)に示すように、ある期間、各装置は、「共通暗号鍵1」を暗号鍵として選択し、それを通信環境に自動設定する。その後、図2

(B)に示すように、ある日時を境に、各装置は、その「共通暗号鍵1」を破棄し、「共通暗号鍵2」を暗号鍵として選択し、それを通信環境に自動設定する。

【0029】つまり、結果として、各装置の暗号鍵が同期的に更新されてセキュリティを高めることができ、かつ、ユーザに暗号鍵の入力や設定等の煩わしい作業を強いることもない。

【0030】図3は、この通信システムを構成する各装置に備えられる暗号鍵更新システムに関わる構成を示すブロック図である。

【0031】なお、この暗号鍵システムに関する構成は、アクセスポイント2およびパーソナルコンピュータ3の双方に同じものが設けられるので、ここでは、パーソナルコンピュータ3を例に説明する。

【0032】パーソナルコンピュータ3は、CPU31、システムメモリ32、フロッピーディスク装置33、磁気ディスク装置34および無線信号送受信装置35を有している。

【0033】CPU31は、パーソナルコンピュータ3全体の制御を司るものであり、無線LAN送受信制御プログラム311、暗号鍵管理プログラム312、アップデートプログラム313等の記述にしたがって、このパーソナルコンピュータ3を動作制御する。

【0034】システムメモリ32は、このパーソナルコンピュータ3の主記憶となるメモリデバイスであり、その時に実際にデータの暗号化および復号に用いられる暗号鍵321を格納するために利用される。

【0035】フロッピーディスク装置33および磁気ディスク装置34は、このパーソナルコンピュータ3の外部記憶となるメモリデバイスであり、フロッピーディスク装置33は、後述する暗号鍵リスト341が格納された頒布用のフロッピーディスクからこれらを読み出すために利用される。一方、磁気ディスク装置34は、フロッピーディスク装置33によりフロッピーディスクから読み出された暗号鍵リスト341を格納するために利用される。この暗号鍵リスト341は、図2を参照しながら説明した、予め複数の暗号鍵が記された暗号鍵リストである。

【0036】そして、無線信号送受信装置35は、データを搬送するための赤外線信号をアクセスポイント2に向けて送信し、あるいは、アクセスポイント2から送信された赤外線信号を受信するためのものである。

【0037】ここで、このパーソナルコンピュータ3が、無線信号送受信装置35を介してアクセスポイント2にデータを送信する場合、および、無線信号送受信装置35を介してアクセスポイント2からデータを受信する場合を考える。

【0038】データを送信する場合、無線LAN送受信制御プログラム311は、システムメモリ32に格納されたいずれかの暗号鍵321を用いてデータを暗号化し、この暗号化されたデータを無線信号送受信装置35を介してアクセスポイント2に送信する。この時、何番目の暗号鍵321を使用したのかを示す情報をパケットに格納しておく。一方、データを受信する場合、無線LAN送受信制御プログラム311は、システムメモリ32に格納された暗号鍵321の中のパケットで指定される番号の暗号鍵321を用いてデータを復号する。

【0039】つまり、このパーソナルコンピュータ3におけるアクセスポイント2との間のデータの送受信では、システムメモリ32に格納された暗号鍵321の管理が非常に重要であることがわかる。

【0040】そこで、次に、暗号鍵管理プログラム312が実行する、この暗号鍵321の更新について説明する。

【0041】まず、図4を参照して、この暗号鍵管理プログラム312による暗号鍵の更新の第1の動作原理を説明する。

【0042】いま、暗号鍵リスト341には、暗号鍵(1)～(n)の複数の暗号鍵が記されており、また、システムメモリ32には、当初、暗号鍵(1)～(4)が暗号鍵321として設定されているものと想定する。

【0043】ある期間の経過後、暗号鍵管理プログラム312は、予め定められた規則に基づき、システムメモリ32の暗号鍵321から既存の暗号鍵(1)と、磁気ディスク装置34の暗号鍵リスト341から暗号鍵(5)～(7)とを選択し、これをシステムメモリ32に新たな暗号鍵321として再設定する。

【0044】さらにある期間の経過後、暗号鍵管理プログラム312は、予め定められた規則に基づき、システムメモリ32の暗号鍵321から既存の暗号鍵(5)と、磁気ディスク装置34の暗号鍵リスト341から暗号鍵(18)～(20)とを選択し、これをシステムメモリ32に新たに暗号鍵321として再設定する。

【0045】同様に、さらにある期間の経過後、暗号鍵管理プログラム312は、予め定められた規則に基づき、システムメモリ32の暗号鍵321から既存の暗号鍵(19)と、磁気ディスク装置34の暗号鍵リスト341から暗号鍵(32)～(34)とを選択し、これを

システムメモリ32に新たに暗号鍵321として再設定する。

【0046】つまり、暗号鍵管理プログラム312は、4つの暗号鍵の中の1つは更新前と更新後とで重複させることにより、この暗号鍵の更新時にデータの送受信を中断させることを防止する。

【0047】なお、この選択時の規則として、暗号鍵管理プログラム312は、暗号鍵リスト341の端から順番に暗号鍵を選択していてもよいが、その順番に不規則性を持たせれば、さらにセキュリティを高めることが可能である。この不規則性を持たせる方法としては、たとえばパーソナルコンピュータ3のシステム時刻を取得し、この取得したシステム時刻をもとに予め定められた関数演算を実行して選択すべき暗号鍵を決定するなどすればよい。

【0048】また、暗号鍵管理プログラム312は、この暗号鍵の更新を予め定められた期間ごとに行ってもよいが、そのサイクルにも不規則性を持たせれば、さらにセキュリティを高めることが可能である。この不規則性を持たせる方法としては、たとえばパーソナルコンピュータ3のシステム時刻を取得し、この取得したシステム時刻をもとに予め定められた関数演算を実行して各暗号鍵の有効期間を決定するなどすればよい。

【0049】次に、図5を参照して、この暗号鍵管理プログラム312による暗号鍵の更新の第2の動作原理を説明する。

【0050】いま、暗号鍵リスト341には、暗号鍵(1)～(n)の複数の暗号鍵が記されており、また、システムメモリ32には、当初、暗号鍵(1)～(2)が暗号鍵321として設定されているものと想定する。つまり、ここでは、一時に設定可能な数であるたとえば4つのうちの半数の2つの暗号鍵を設定する。

【0051】ある期間の経過後、暗号鍵管理プログラム312は、予め定められた規則に基づき、磁気ディスク装置34の暗号鍵リスト341から暗号鍵(5)～(6)を選択し、これをシステムメモリ32に新たな暗号鍵321として再設定する。

【0052】これに伴い、無線LAN送受信制御プログラム311は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵(5)～(6)の2つとする。しかし、無線LAN送受信制御プログラム311は、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵(5)～(6)の2つに更新前の暗号鍵(1)～(2)を加えた合計4つとする。

【0053】さらにある期間の経過後、暗号鍵管理プログラム312は、予め定められた規則に基づき、磁気ディスク装置34の暗号鍵リスト341から暗号鍵(18)～(19)を選択し、これをシステムメモリ32に新たな暗号鍵321として再設定する。これに伴い、無

線LAN送受信制御プログラム311は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵(18)～(19)の2つとし、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵(18)～(19)の2つに更新前の暗号鍵(5)～(6)を加えた合計4つとする。

【0054】同様に、さらにある期間の経過後、暗号鍵管理プログラム312は、予め定められた規則に基づき、磁気ディスク装置34の暗号鍵リスト341から暗号鍵(32)～(33)を選択し、これをシステムメモリ32に新たな暗号鍵321として再設定し、無線LAN送受信制御プログラム311は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵(32)～(33)の2つとするとともに、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵(32)～(33)の2つに更新前の暗号鍵(18)～(19)を加えた合計4つとする。

【0055】つまり、暗号鍵管理プログラム312は、暗号鍵の更新を更新前と更新後とで重複することなく実行するが、無線LAN送受信制御プログラム311が、更新前の暗号鍵を予め定められた期間内に限り許容することにより、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収する。そして、このために、暗号鍵管理プログラム312は、暗号鍵の設定数を一時に取り扱い可能な数の半数以下とする。

【0056】このように、この暗号鍵更新システムでは、たとえば1年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたことにより、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とする。

【0057】次に、図6および図7を参照して、この暗号鍵更新システムの動作手順を説明する。

【0058】図6は、暗号鍵管理プログラム312の動作手順を説明するためのフローチャートである。

【0059】暗号鍵管理プログラム312は、まず、このパーソナルコンピュータ3のシステム時刻を取得する(ステップA1)。システム時刻を取得すると、暗号鍵管理プログラム312は、その取得したシステム時刻をもとに暗号鍵選択用に予め与えられた関数演算を実行し、磁気ディスク装置34に格納された暗号鍵リスト341の中から新たな暗号鍵を選択する(ステップA2)。

【0060】新たな暗号鍵を選択すると、暗号鍵管理プログラム312は、その選択した暗号鍵をシステムメモリ32に暗号鍵321として設定する(ステップA3)。そして、暗号鍵管理プログラム312は、先に取

得したシステム時刻をもとに有効期間算出用に予め与えられた関数演算を実行し、この新たな暗号鍵の有効期間を算出する(ステップA4)。

【0061】最後に、暗号鍵管理プログラム312は、その算出した有効期間後に自身を再起動するための起動タイマを設定し(ステップA5)、この処理を終了する。

【0062】図7は、無線LAN送受信制御プログラム311の復号時における動作手順を説明するためのフローチャートである。

【0063】無線LAN送受信制御プログラム311は、無線信号送受信装置35を介してアクセスポイント2からのデータを受信すると、システムメモリ32に設定された暗号鍵の中のバケットで指定された番号の暗号鍵を用いてこのデータの復号を試みる(ステップB1)。

【0064】この復号が成功すると(ステップB2のYES)、無線LAN送受信制御プログラム311による復号処理は終了であるが、一方、失敗すると(ステップB2のNO)、無線LAN送受信制御プログラム311は、システムメモリ32に設定された暗号鍵321の更新から予め定められた期間内かどうかを調べる(ステップB3)。

【0065】予め定められた期間内であれば(ステップB3のYES)、無線LAN送受信制御プログラム311は、今度は、更新前の旧暗号鍵の中のバケットで指定された番号の旧暗号鍵を用いてこのデータの復号を試みる(ステップB4)。

【0066】そして、復号が成功すれば(ステップB7のYES)、無線LAN送受信制御プログラム311による復号処理は終了となり、一方、失敗するか(ステップB5のNO)、あるいは、暗号鍵321の更新から予め定められた期間内でなかったとき(ステップB3のNO)、無線LAN送受信制御プログラム311は、アクセスポイント2にエラー返答を通知する(ステップB6)。

【0067】なお、この図7で示した無線LAN送受信制御プログラム311の復号時における動作手順は、暗号鍵管理プログラム312が図5に示した第2の動作原理で暗号鍵を更新する場合のものであり、暗号鍵管理プログラム312が図4に示した第1の動作原理で暗号鍵を更新する場合には、ステップB2における復号が失敗した時点で、ステップB6のエラー返答の通知を行えばよい。

【0068】ところで、この暗号鍵リスト341を配布してシステムを起動させた後は、この暗号鍵リスト341自体を暗号化して授受することができるようになる。したがって、これ以降は、頒布用のフロッピーディスクに暗号鍵リスト341を格納して配布し、各装置側でフロッピーディスク装置33により読み出して設定するな

どといったことを一切不要とすることが可能となる。そして、そのために、この暗号鍵更新システムでは、アップデートプログラム313を準備する。

【0069】ネットワーク管理サーバコンピュータ1から送信される暗号鍵リストが無線信号送受信部装置35により受信されると、まず、無線LAN送受信制御プログラム311が、アクセスポイント2によって暗号化された暗号鍵リストの復号を実行する。そして、この復号された暗号鍵リストは、アップデートプログラム313に転送され、アップデートプログラム313によって、磁気ディスク装置34の暗号鍵リスト341の更新が実行される。

【0070】また、セキュリティをより高めるために、このアップデートプログラム313に、暗号鍵管理プログラム312の更新機能をもたせることも有効である。つまり、ネットワーク管理サーバコンピュータ1から暗号化された新たな暗号鍵管理プログラムを送信し、この暗号化された新たな暗号鍵管理プログラムを無線LAN送受信制御プログラム311に復号させた後、アップデートプログラム313に暗号鍵管理プログラム312の更新を実行させる。これにより、暗号鍵の選択規則も入手を介さずに更新できることになり、かつ、暗号が破られる危険性を低くすることが可能となる。

【0071】

【発明の効果】以上、詳述したように、この発明によれば、たとえば1年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたため、その結果として、すべての装置が同期を取って暗号鍵を自動的に更新することが可能となり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることがない。

【0072】また、暗号鍵の更新サイクルに不規則性を持たせることにより、セキュリティをより向上させることが可能となる。

【0073】さらに、たとえば更新前と更新後とで暗号鍵を少なくとも1つは重複させ、あるいは、予め定めら\*

\*れた期間内に限り更新前の暗号鍵を復号用の暗号鍵の候補に加えることにより、暗号鍵の更新時にもデータの送受信を中断させることを防止し、あるいは、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収することを可能とする。

【図面の簡単な説明】

【図1】この発明の実施形態に係る暗号鍵更新システムが適用される通信システムのネットワーク構成図。

【図2】同実施形態の暗号鍵更新システムで実行される暗号鍵の更新の概要を示すための概念図。

【図3】同実施形態の通信システムを構成する各装置に備えられる暗号鍵更新システムに関わる構成を示すブロック図。

【図4】同実施形態の暗号鍵管理プログラムによる暗号鍵の更新の第1の動作原理を説明するための図。

【図5】同実施形態の暗号鍵管理プログラムによる暗号鍵の更新の第2の動作原理を説明するための図。

【図6】同実施形態の暗号鍵管理プログラムの動作手順を説明するためのフローチャート。

【図7】同実施形態の無線LAN送受信制御プログラムの復号時における動作手順を説明するためのフローチャート。

【符号の説明】

1…ネットワーク管理サーバコンピュータ

2…アクセスポイント

3…パーソナルコンピュータ

31…CPU

32…システムメモリ

33…フロッピーディスク

34…磁気ディスク装置

35…無線信号送受信装置

100…有線LAN

311…無線LAN送受信制御プログラム

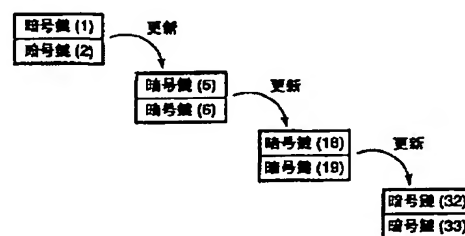
312…暗号鍵管理プログラム

313…アップデートプログラム

321…暗号鍵

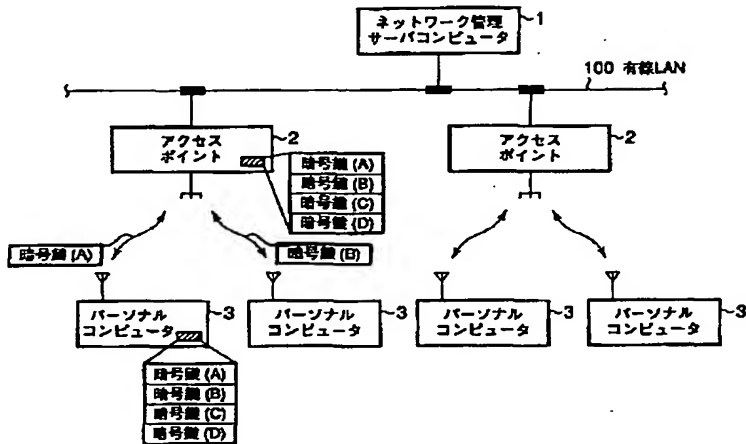
341…暗号鍵リスト

【図5】

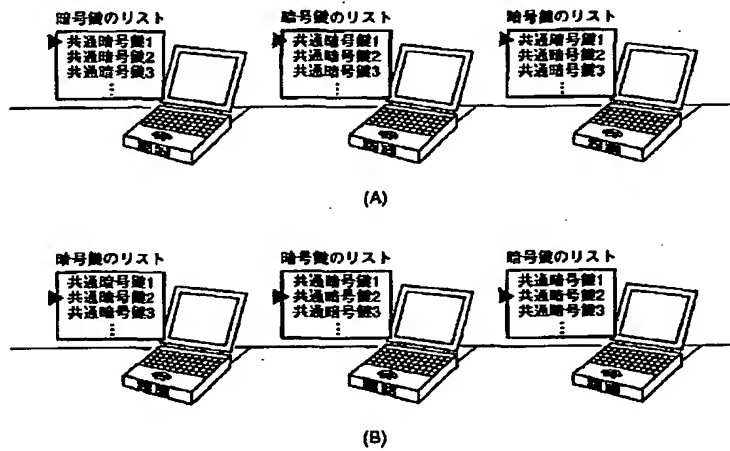




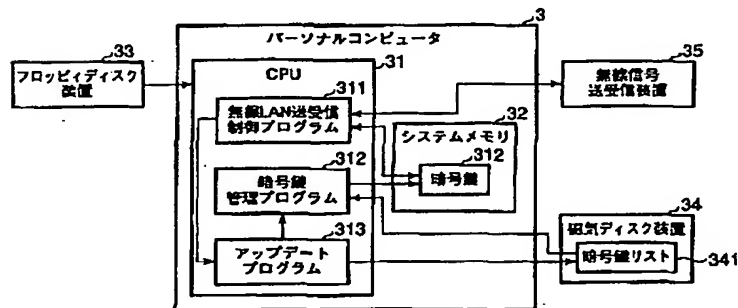
【図1】



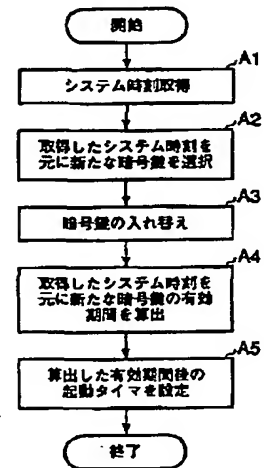
【図2】



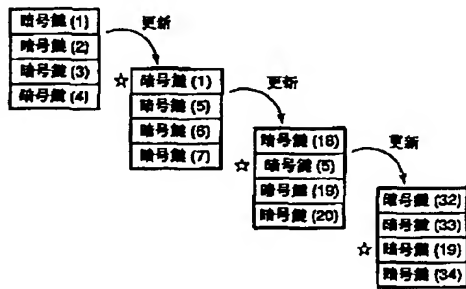
【図3】



【図6】



【図4】



【図7】

